

## **REMARKS**

Applicants respectfully request consideration of the subject application. Applicants amended claims 6 and 30 to clarify the limitations already present in the claims, thus Applicants added no new matter through the amendments.

### **Claim Rejections under 35 U.S.C. § 103(a)**

Claims 1-15 and 25-34 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over Blaker, et al. U.S. Publication No. 2002/0004904 ("Blaker") in view of U.S. Patent No. 6,584,567 to Bellwood ("Bellwood") and in view of U.S. Publication No. 2002/0146128 to Mauro et al ("Mauro").

Claims 16-18, 20-22, and 24 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over Blaker in view of Mauro.

Claims 19 and 23 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over Blaker in view of Mauro and further in view of U.S. Patent No. 5,925,123 to Tremblay ("Tremblay").

### **Claims 1-15 and 25-34**

#### ***Claim 1***

Claim 1 requires calling with a *single* macro instruction operation from a first processor, the *single* macro instruction operation representing a *plurality* of primitive security operations. Moreover, claim 1 requires executing the *plurality* of primitive security operations at a second processor in response to receiving the *single* macro instruction operation from the first processor.

By way of example and not limitation, the specification in paragraph [0024] discloses a primitive security operation can be a decrypt operation, an encrypt operation, a hash operation, or a group of arithmetic operations.

Blaker describes a command block created by a host processor. The command block includes commands for execution, locations for storing, and parameters to be loaded by the cryptographic accelerator processor. Blaker describes a one to one relationship between operand to instruction. For instance, paragraph 11 describes, “one or more operands are downloaded into the local memory from the system memory and the cryptographic processor executes an instruction that references one of the downloaded operands.” (Blaker, para. 11, emphasis added). Thus, for every operand in the command block the cryptographic accelerator processor executes one instruction.

Therefore, Blaker fails to describe or suggest executing the plurality of primitive security operations at a second processor in response to receiving the single macro instruction operation from the first processor.

Bellwood describes a method of enabling a proxy to participate in a secure communication between a client and a set of servers. (Bellwood, Abstract). A first secure connection is established between the client and the proxy. (Bellwood, Abstract). The method also describes the proxy participating in secure communications between the client and a first server. (Bellwood, Abstract).

Bellwood fails to describe or suggest executing the plurality of primitive security operations at a second processor in response to receiving the single macro instruction operation from the first processor.

Mauro describes a DSP performing a primitive cryptographic function when the CPU sends a command and/or many executable instructions to execute one primitive cryptographic function on the DSP. Specifically, Mauro describes “when a primitive cryptographic function is required, the CPU downloads the DSP assembly image into the DSP” and sends a command to the DSP to execute the primitive cryptographic function. (Mauro, para. [0029]). This image contains the DSP executable instructions (microcode) “required to execute the particular primitive cryptographic function.” (Mauro, para. [0029]). The CPU then sends a command to the DSP to execute the particular primitive function. (Mauro, para. [0029]). Mauro also describes the above one command to execute one primitive cryptographic function for the following primitive cryptographic functions: hash (para. [0033]), modular exponentiation (paras. [0031], [0037]; Figure 3), encryption/decryption (paras. [0034], [0040], [0041]; Figure 5; Figure 6), and modular math (para. [0039]; Figure 4). Thus, the CPU sends one command and/or executable instructions to perform one primitive cryptographic function.

For example, Mauro describes using the DSP to accelerate the modular exponentiation used in Diffie-Hellman and RSA key exchange algorithms. (Mauro, paras. [0031], [0037]). The CPU downloads the executable instructions that cause the DSP to execute the exponentiation function which is a primitive cryptographic function. (Mauro, para. [0031], [0037]). Thus, Mauro describes using a command and/or many executable instructions to perform one primitive cryptographic function.

Conversely, claim 1 requires executing the plurality of primitive security operations at a second processor in response to receiving the single macro

instruction operation from the first processor.

Because Mauro describes using a command and/or many executable instructions to perform one primitive cryptographic function, Mauro fails to describe or suggest calling with a single macro instruction operation from a first processor, executing the plurality of primitive security operations at a second processor in response to receiving the single macro instruction operation from the first processor.

Because Blaker, Bellwood, and Mauro each fail to describe or suggest executing the plurality of primitive security operations at a second processor in response to receiving the single macro instruction operation from the first processor, the combination of Blaker, Bellwood, and Mauro fails to describe or suggest the above limitation. As such, the combination of Blaker, Bellwood, and Mauro fails to render claim 1 obvious.

#### *Claims 2-5*

Applicants respectfully submit that claims 2-5 are dependent on claim 1; therefore, claims 2-5 include the same limitations as claim 1. As such, claims 2-5 are patentable for at least the same reasons as claim 1.

#### *Claim 6*

Claim 6 as amended requires similar limitations as claim 1. Specifically, claim 6 requires calling a macro security operation from a first processor to a second processor, the macro security operation representing a set of primitive security operations and performing the set of primitive security operations in response to the macro security operation.

Thus for at least the same reasons discussed for claim 1, the combination of Blaker, Bellwood, and Mauro fails to describe or suggest performing the set of primitive security operations in response to the macro security operation; therefore, the combination fails to describe or suggest the above limitation. As such, the combination of Blaker, Bellwood, and Mauro fails to render claim 6 obvious for at least the reasons discussed for claim 1.

Furthermore, claim 6 requires a set of primitive security operations comprising, generating a secret and a key material, creating a first finished hash for a client message, creating a second finished hash for a server message, and creating a finished message.

#### *Claims 7-10*

Applicants respectfully submit that claims 7-10 are dependent on claim 6; therefore, claims 7-10 include the same limitations as claim 6. As such, claims 7-10 are patentable for at least the same reasons as claim 6.

#### *Claim 11*

Claim 11 requires similar limitations as claim 1. Specifically, claim 11 requires the second network element to call a macro security operation from a first processor, the macro security operation associated with a plurality of primitive security operations and to execute the plurality of primitive security operations at a second processor in response to the macro security operation.

Thus for at least the same reasons discussed for claim 1, the combination of Blaker, Bellwood, and Mauro fails to describe or suggest the macro security operation associated with a plurality of primitive security operations and to execute the plurality of primitive security operations at a second processor in response to the macro security operation; therefore, the combination fails to describe or suggest the above limitation. As such, the combination of Blaker, Bellwood, and Mauro fails to render claim 11 obvious for at least the reasons discussed for claim 1.

#### *Claims 12-15*

Applicants respectfully submit that claims 12-15 are dependent on claim 11; therefore, claims 12-15 include the same limitations as claim 11. As such, claims 12-15 are patentable for at least the same reasons as claim 11.

#### *Claims 25*

Claim 25 requires similar limitations as claim 1. Specifically, claim 25 requires executing a macro security operation at a first one of the set of processors, the macro security operation associated with a plurality of primitive security operations and executing a plurality of primitive security operations at a second one of the set of processors in response to the macro security operation.

Thus for at least the same reasons discussed for claim 1, the combination of Blaker, Bellwood, and Mauro fails to describe or suggest executing a plurality of primitive security operations at a second one of the set of processors in response to the macro security operation; therefore, the combination fails to describe or suggest

the above limitation. As such, the combination of Blaker, Bellwood, and Mauro fails to render claim 25 obvious for at least the reasons discussed for claim 1.

#### *Claims 26-29*

Applicants respectfully submit that claims 26-29 are dependent on claim 25; therefore, claims 26-29 include the same limitations as claim 25. As such, claims 26-29 are patentable for at least the same reasons as claim 25.

#### *Claim 30*

Claim 30 as amended requires similar limitations as claim 1. Specifically, claim 30 requires calling a macro security operation from a first one of the set of processors, the macro security operation associated with a set of primitive security operations and performing the set of primitive security operations at a second one of the set of processors in response to the macro security operation.

Thus for at least the same reasons discussed for claim 1, the combination of Blaker, Bellwood, and Mauro fails to describe or suggest performing the set of operations at a second one of the set of processors in response to the macro security operation; therefore, the combination fails to describe or suggest the above limitation. As such, the combination of Blaker, Bellwood, and Mauro fails to render claim 30 obvious for at least the reasons discussed for claim 1.

Furthermore, claim 30 requires a set of primitive security operations comprising, generating a secret and a key material, creating a first finished hash for a client message, creating a second finished hash for a server message, and creating a finished message.

### *Claims 31-34*

Applicants respectfully submit that claims 31-34 are dependent on claim 30; therefore, claims 31-34 include the same limitations as claim 30. As such, claims 31-34 are patentable for at least the same reasons as claim 30.

### *Claims 16-24*

#### *Claim 16*

Claim 16 requires a first processor to call a macro security operation associated with a plurality of primitive security operations. Moreover, claim 16 further requires a second processor to perform the plurality of primitive security operations in response to the macro security operation from said first processor.

As discussed above, Blaker describes a one to one relationship between operand to instruction, thus fails to describe or suggest a second processor to perform the plurality of primitive security operations in response to the macro security operation from said first processor.

Mauro, also discussed above, describes a CPU that sends a command and/or executable instructions to perform one primitive cryptographic function. Therefore, Mauro fails to describe or suggest to perform the plurality of primitive security operations in response to the macro security operation from said first processor.

Because Blaker and Mauro fail to describe or suggest a second processor to perform the plurality of primitive security operations in response to the macro



security operation from said first processor, the combination of Blaker and Mauro fails to describe or suggest the above limitation. As such, the combination of Blaker and Mauro fails to render claim 16 obvious.

#### *Claims 17-20*

Applicants respectfully submit that claims 17-20 are dependent on claim 16; therefore, claims 17-20 include the same limitations as claim 16. As such, claims 17-20 are patentable for at least the same reasons as claim 16.

#### *Claim 21*

Claim 21 requires similar limitations as claim 16. Specifically, claim 21 requires a first processor to give the command for a macro security operation associated with a plurality of primitive security operations. Moreover, claim 21 requires a request unit to retrieve the macro security operation associated with the plurality of primitive security operations. Another requirement of claim 21 includes one of a plurality of execution units to perform the plurality of primitive security operations retrieved by the request unit, the plurality of primitive security operations corresponding to the macro security operation.

Thus for at least the same reasons discussed for claim 16, the combination of Blaker and Mauro fails to describe or suggest a first processor to give the command for a macro security operation associated with a plurality of primitive security operations, a request unit to retrieve the macro security operation associated with the plurality of primitive security operations, and one of a plurality of execution units

to perform the plurality of primitive security operations corresponding to the macro security operation; therefore, the combination fails to describe or suggest the above limitation. As such, the combination of Blaker and Mauro fails to render claim 20 obvious for at least the reasons discussed for claim 16.

#### *Claims 22-24*

Applicants respectfully submit that claims 22-24 are dependent on claim 21; therefore, claims 22-24 include the same limitations as claim 21. As such, claims 22-24 are patentable for at least the same reasons as claim 21.

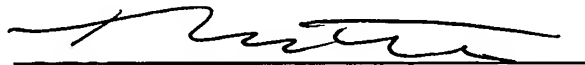
Conclusion

If the allowance of these claims could be facilitated by a telephone conference, the Examiner is invited to contact Daniel De Vos at (408) 720-8300. If there are any additional charges, please charge our Deposit Account No. 02-2666.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

Dated: June 2, 2006



Thomas C. Webster  
Registration No. 46,154

Customer No. 08791  
12400 Wilshire Boulevard  
Seventh Floor  
Los Angeles, CA 90025-1030  
(408) 720-8300